Post GDPR enforcement in Germany — a sneak peek

Benjamin Beck, Associate, and Ulrich Worm, Partner, Mayor Brown, discuss the GDPR enforcement action that has been taken across German states since the Regulation came into effect

German Supervisory Authorities have issued 41 fines since the EU General Data Protection Regulation ('GDPR') became enforceable in May 2018. The highest fine in a single case was EUR 80,000, and the majority of fines (33) originated from the state of North-Rhine Westphalia.

Fines were levied for a variety of GDPR violations, such as inadequate technical and organisational security measures, non-compliance with information duties and sending unauthorised marketing e-mails. The highest fine of EUR 80,000, which originated from the state of Baden-Württemberg, related to sensitive health data being made available on the internet due to inadequate security measures.

First GDPR non-compliance fine

The first GDPR non-compliance fine in Germany was issued on 21st November 2018. The Supervisory Authority of Baden-Württemberg imposed a fine of EUR 20,000 against a German social media provider for failing to encrypt user passwords. Email addresses and passwords of about 330,000 users of the provider's social media website were hacked and published on the internet.

The provider notified the Supervisory Authority of the personal data breach and provided extensive information concerning its data processing activities. From the information supplied to it, the authority learned that user passwords were stored unencrypted.

Pursuant to Article 32 of the GDPR, companies must implement appropriate technical and organisational measures to secure personal data so that the rights and freedoms of the concerned natural persons are protected. To determine the appropriate measures, organisations must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing the personal data.

Based on those considerations — and the fact that encryption of personal data is listed as an appropriate measure in Article 32(1)(a) of the GDPR — the Supervisory Authority of Baden-Württemberg determined that the social media provider should have encrypted user passwords rather than processing them in plain text, to grant a level of protection appropriate to the risks. Consequently, the authority concluded that the provider had violated Article 32(1)(a) of the GDPR and applied a fine pursuant to Article 83(4).

The authorities' fine could have been as high as EUR 10 million or 2% of the company's worldwide turnover of the previous year, whichever is higher. However, when determining the amount of the fine, the Supervisory Authority of Baden-Württemberg considered the efforts taken by the provider to implement the measures ordered and suggested by the authority and the provider's willingness to cooperate with the authority.

Complaints reported by data subjects

Reportedly, the German Supervisory Authorities learned about most GDPR violations not from their own investigations, but from data subjects reporting them to the authorities.

Pursuant to Article 77 of the GDPR, every data subject has the right to lodge a complaint with a Supervisory Authority if the data subject believes that the processing of personal data relating to him or her infringes the GDPR. According to statistics provided by the Supervisory Authority of the state of Baden-Württemberg, the number of complaints from data subjects was thirty percent higher in 2018 as compared to 2017.

Other German authorities seem to have had similar experiences in recent months. For example, the Supervisory Authority for the state of Rhineland-Palatinate reportedly receives more than 200 calls on a daily basis. The one for Thuringia claims to have received 500 emails per day during the first months since the GDPR became enforceable.

These numbers point towards at least two conclusions: first, data subjects have become more aware of their rights under the GDPR—and they are willing to enforce them.

Second, there are many uncertainties about the implementation of the GDPR. For example, even the legality of having nameplates on doorbells or sending out corporate holiday cards was called into question.

A look ahead

In most cases, the Supervisory Authorities applied sanctions other than fines, such as conducting investigations and on-site audits, or issuing warnings or reprimands. Only some GDPR violations were sanctioned with a fine also because most authorities granted grace periods, during which fines were set at lower amounts than they could or should have been, or were not issued at all.

However, grace periods should not be relied on, because it is unclear whether and for how long they will be applied by the authorities. Further, it is important to keep in mind that fines can be substantial: the maximum fine under the GDPR may reach EUR 20 million or 4% of the total worldwide annual turnover of the preceding financial year (whichever is higher), depending on the type and extent of the GDPR violation.

An increasing number of fines from German Supervisory Authorities is to be expected soon. For example, reportedly, the Supervisory Authority for the state of Bavaria is currently dealing with 85 pending fine proceedings.

Benjamin Beck and Ulrich Worm
Mayer Brown
uworm@mayerbrown.com
bbeck@mayerbrown.com

Effective record-keeping is a crucial part of Compliance

pdp TRAINING

We've designed three highly practical training sessions to ensure Compliance Professionals have the Records Management skills they require for their roles

Records Management Level 1

Records Management Level 2

Advanced Records Management

Each course has availability at locations around the UK in 2019

For more information, go online or contact our training team on +44 (0)207 014 3399

www.pdptraining.com